GAO Highlights

March 25, 2014

INFORMATION SECURITY

VA Needs to Address Long-Standing Challenges

Why GAO Did This Study

The use of information technology is crucial to VA's ability to carry out its mission of ensuring that veterans receive medical care, benefits, social support, and memorials. However, without adequate security protections, VA's systems and information are vulnerable to exploitation by an array of cyber-based threats, potentially resulting in, among other things, the compromise of veterans' personal information. GAO has identified information security as a government-wide high-risk area since 1997. The number of information security incidents reported by VA has more than doubled over the last several years, further highlighting the importance of securing the department's systems and the information that resides on them.

GAO was asked to provide a statement discussing the challenges VA has experienced in effectively implementing information security, as well as to comment on a recently proposed bill aimed at improving the department's efforts to secure its systems and information. In preparing this statement GAO relied on previously published work as well as a review of recent VA inspector general and other reports related to the department's security program. GAO also analyzed the draft legislation in light of existing federal requirements and best practices for information security.

What GAO Found

The Department of Veterans Affairs (VA) continues to face long-standing challenges in effectively implementing its information security program. Specifically, from fiscal year 2007 through 2013, VA has consistently had weaknesses in key information security control areas (see table).

Control Weaknesses for Fiscal Years 2007-2013

Security control category	2007	2008	2009	2010	2011	2012	2013
[illegible]	✓	✓	✓	✓	✓	✓	✓
[illegible]	✓	✓	✓	✓	✓	✓	✓
[illegible]	✓	✓	✓	✓	✓	✓	✓
[illegible]	✓	✓	✓	✓	✓	✓	✓
[illegible]	✓	✓	✓	✓	✓	✓	✓

Source: GAO analysis based on VA and inspector general reports.

In addition, in fiscal year 2013, the department's independent auditor reported, for the 12th year in a row, that weaknesses in information system controls over financial systems constituted a material weakness. Further, the department's inspector general has identified development of an effective information security program and system security controls as a major management challenge for VA. These findings are consistent with challenges GAO has identified in VA's implementation of its security program going back to the late 1990s. More recently, GAO has reported and made recommendations on issues regarding the protection of personally identifiable information at federal agencies, including VA. These were related to developing and implementing policies and procedures for responding to data breaches, and implementing protections when engaging in computerized matching of data for the purposes of determining individuals' eligibility for federal benefits.

Draft legislation being considered by the Subcommittee addresses the governance of VA's information security program and security controls for the department's systems. It would require the Secretary of VA to improve transparency and coordination of the department's security program and ensure the security of its critical network infrastructure, computers and servers, operating systems, and web applications, as well as its core veterans health information system. Toward this end, the draft legislation prescribes specific security-related actions. Many of the actions and activities specified in the bill are sound information security practices and consistent with federal guidelines. If implemented on a risk-based basis, they could prompt VA to refocus its efforts on steps needed to improve the security of its systems and information. At the same time, the constantly changing nature of technology and business practices introduces the risk that control activities that are appropriate in the department's current environment may not be appropriate in the future. In light of this, emphasizing that actions should be taken on the basis of risk may provide the flexibility needed for security practices to evolve as changing circumstances warrant and help VA meet the security objectives in the draft legislation.